AFN, INC.

February 6, 2006

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street SW
Washington, D.C. 20554

Re: Certification of CPNI Filing (February 6, 2006)
EB-06-TC-060
EB Docket No. 06-36

Dear Ms. Dortch:

Enclosed please find American Fiber Network, Inc.'s ("AFN") Complicance Certificate as required by 47 C.F.R. §64.2009(e), for the period January 1, 2005-December 31, 2005, along with the Company's accompanying statement explaining how its operating procedures ensure compliance with the rules.

Sincerely,

s/Robert E. Heath
Robert E. Heath
EVP
American Fiber Network, Inc.

Attachment

Cc: Byron McCoy, Enforcement Bureau (via email)
Best Copy and Printing (via email)

American Fiber Network, Inc.'s Compliance Certification

February 6, 2006

I certify as an officer of American Fiber Network, Inc.; that I have personal knowledge that American Fiber Network, Inc. has established operating procedures that are adequate to ensure compliance with the Federal Communications Commission requirements as it pertains to Customer Proprietary Network Information, 47 C.F.R. §64.2009(e).

PRINTED NAME Douglas C. Bethell

POSITION CEO

SIGNATURE s/Douglas C. Bethell

DATE 2-3-06

American Fiber Network, Inc.'s Compliance Statement Regarding CPNI

For the Period January 1, 2005-December 31, 2005

Compliance with 47 C.F.R § 64.2001-2009

Notice and Approval.

AFN is in compliance with the rules requiring notice and approval to use customer proprietary network information (CPNI). AFN's processes require that new customers signed a CPNI use authorization. This authorization is kept on file in AFN's offices in both paper and electronic form. AFN does not conduct marketing campaigns that use CPNI. If it did, AFN would not use the CPNI of those customers who withheld approval.

Protecting Confidentiality.

AFN maintains the security of CPNI. AFN has security measures in place to protect this data from:

- external attacks to its network,
- improper use of web portals provided to wholesale and retail customers,
- improper use of FTP (file transfer protocol) sites where customers can obtain data, and
- improper verbal requests for data via personal contacts with AFN's Customer Care.

All of AFN's network equipment and servers are located in facilities where AFN maintains the physical security of the building. At a network level, AFN employs several firewalls to secure the infrastructure and management of its network. AFN also uses secure ID technology for access to its local area network (LAN). AFN's network equipment is behind additional firewalls on its own dedicated network with limited employee access.

AFN's web portals allow toll data to be viewed and downloaded by our retail customers. It has login/password security and uses encryption to ensure the security of this information. The web portal allows customers to only access their specific toll records. AFN's FTP site allows wholesale customers to obtain their specific toll records. AFN's web portal and FTP sites uses standard industry security and current state of the art firewall architecture. AFN has procedures in place in its Customer Care division that allow only customers of record to obtain their specific call detail information. AFN has a code of conduct and training for all employees concerning the se and handling of CPNI, and provides strict disciplinary measures for violations of the code. AFN does not provide CPMO to non-affiliated third parties and does not sell CPNI.